

FIG. 1 is a block diagram of a computer system 100. The computer system 100 includes a processor 102, a memory 104, a read only memory 106, a mass storage device 107, a display 121, a keyboard 122, a cursor control device 123, and a communication device 125. The processor 102 is connected to the memory 104, the read only memory 106, and the mass storage device 107 via a bus 101. The processor 102 is also connected to the display 121, the keyboard 122, the cursor control device 123, and the communication device 125 via a bus 101. The computer system 100 is connected to a network 110 via a communication device 125.

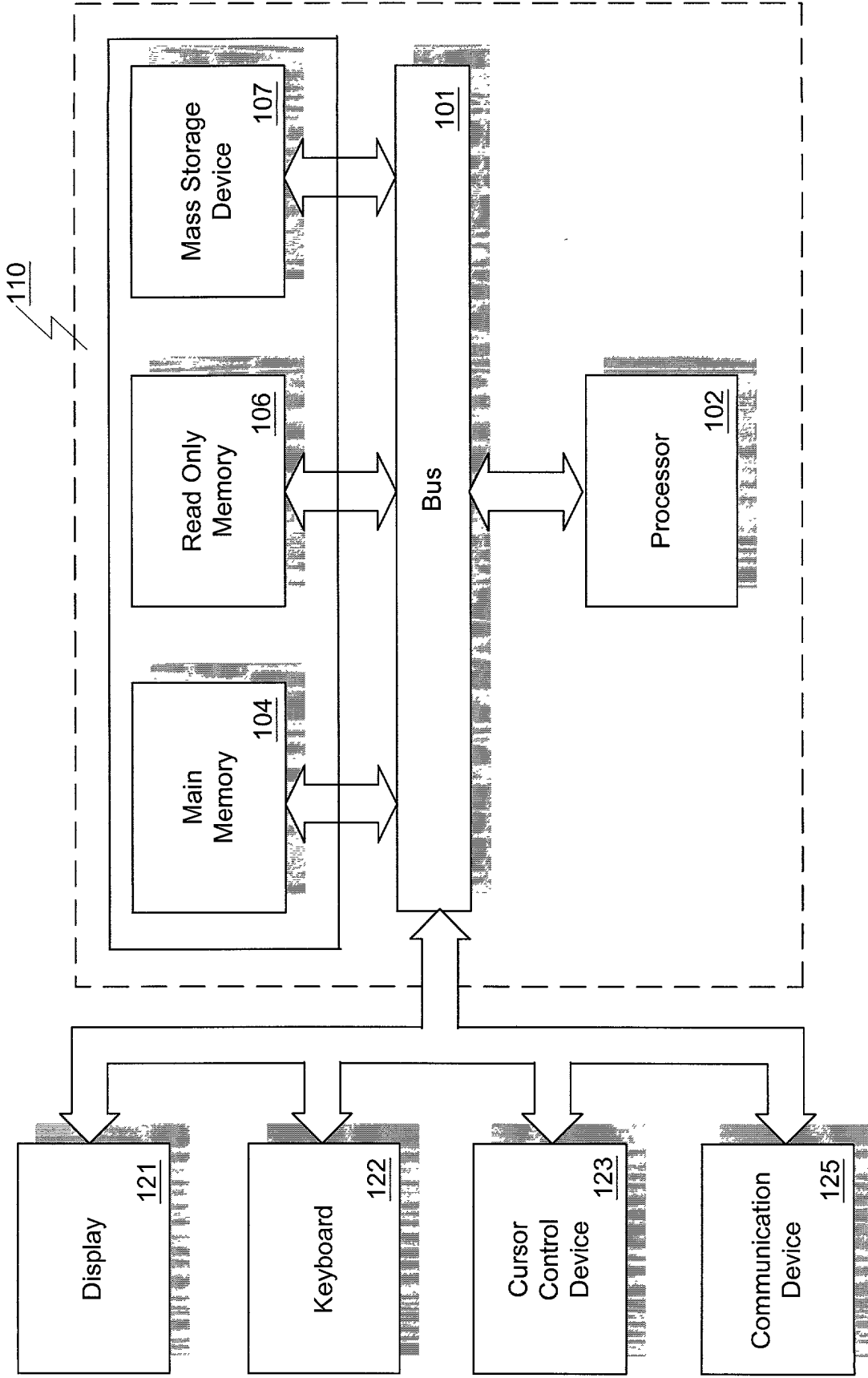


Figure 1

FIG. 2 is a block diagram of a network system. The network system includes a local system 220 and a network 210. The local system 220 is connected to the network 210. The network 210 is an Ethernet TCP/IP network. The network 210 includes a remote independent system (entropy server) 230 and a remote independent system (entropy server) 240.

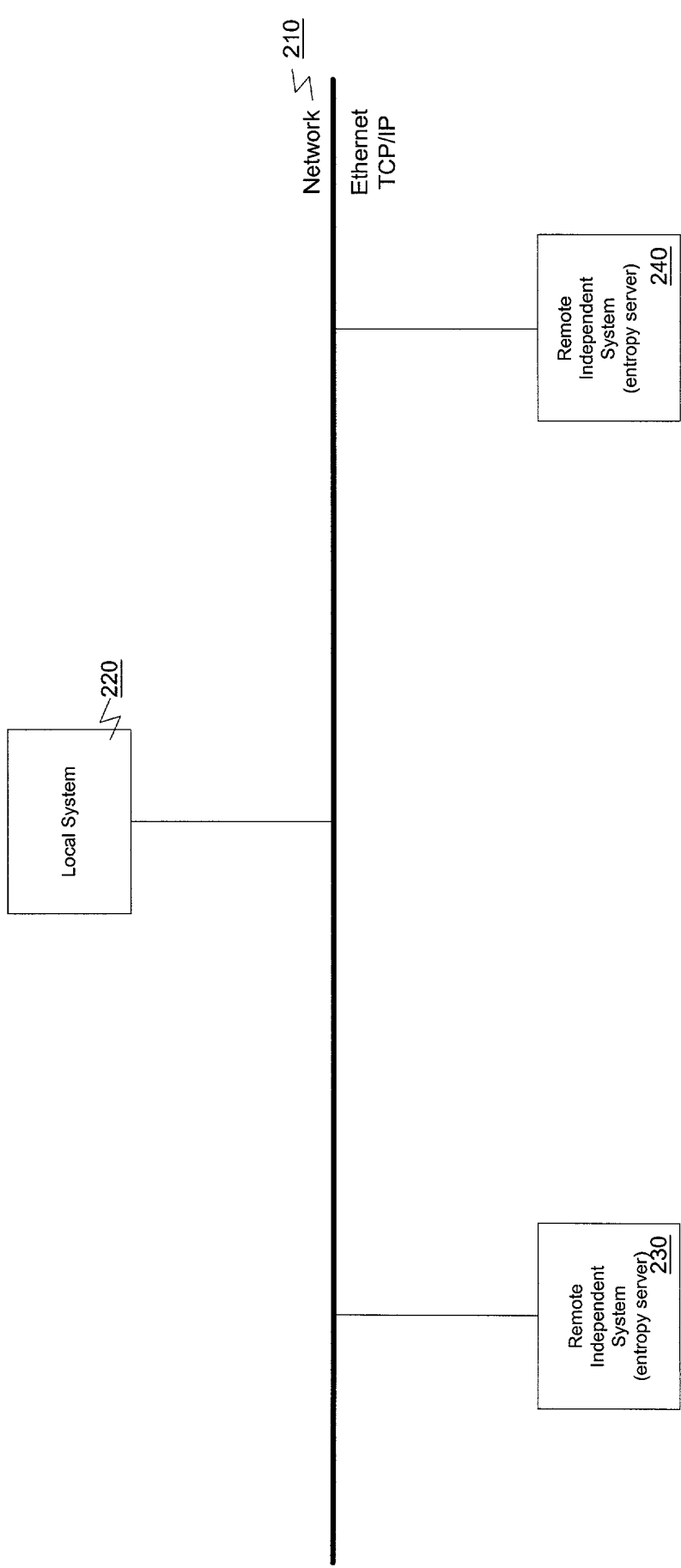


Figure 2

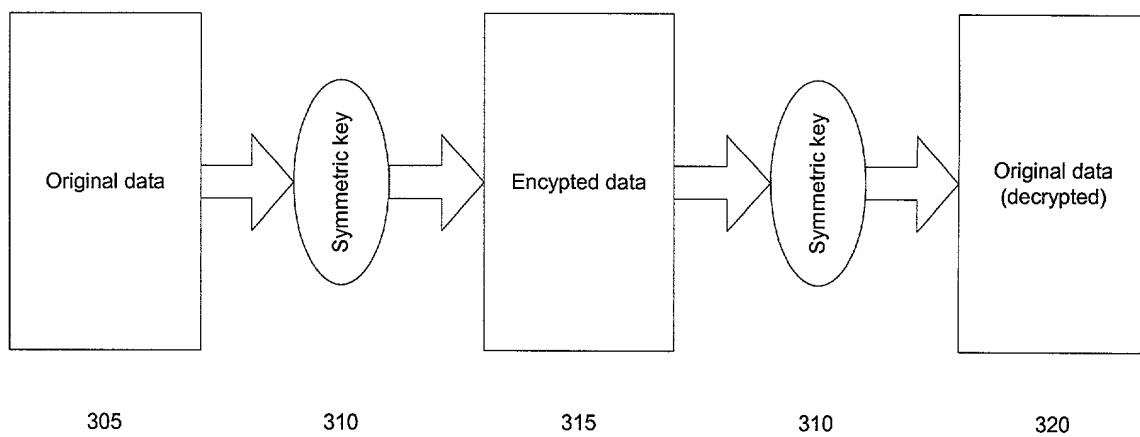


Figure 3A

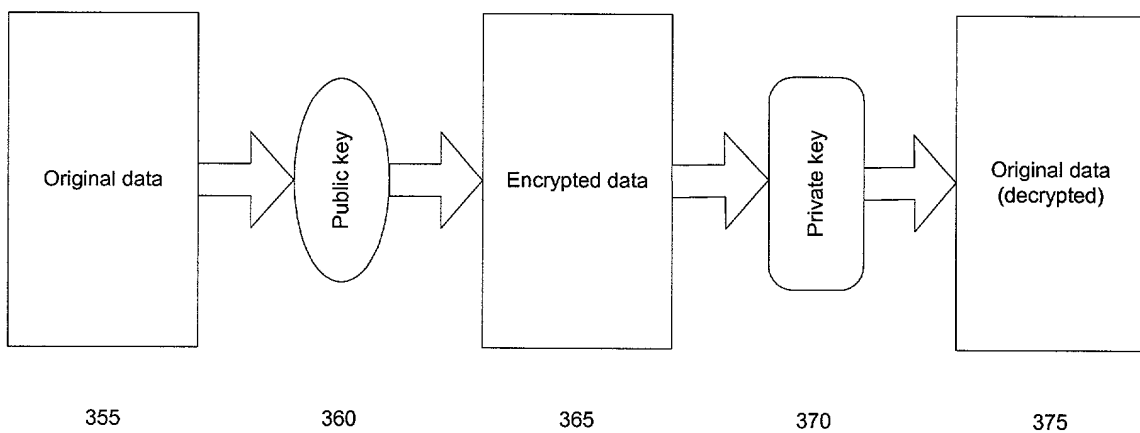
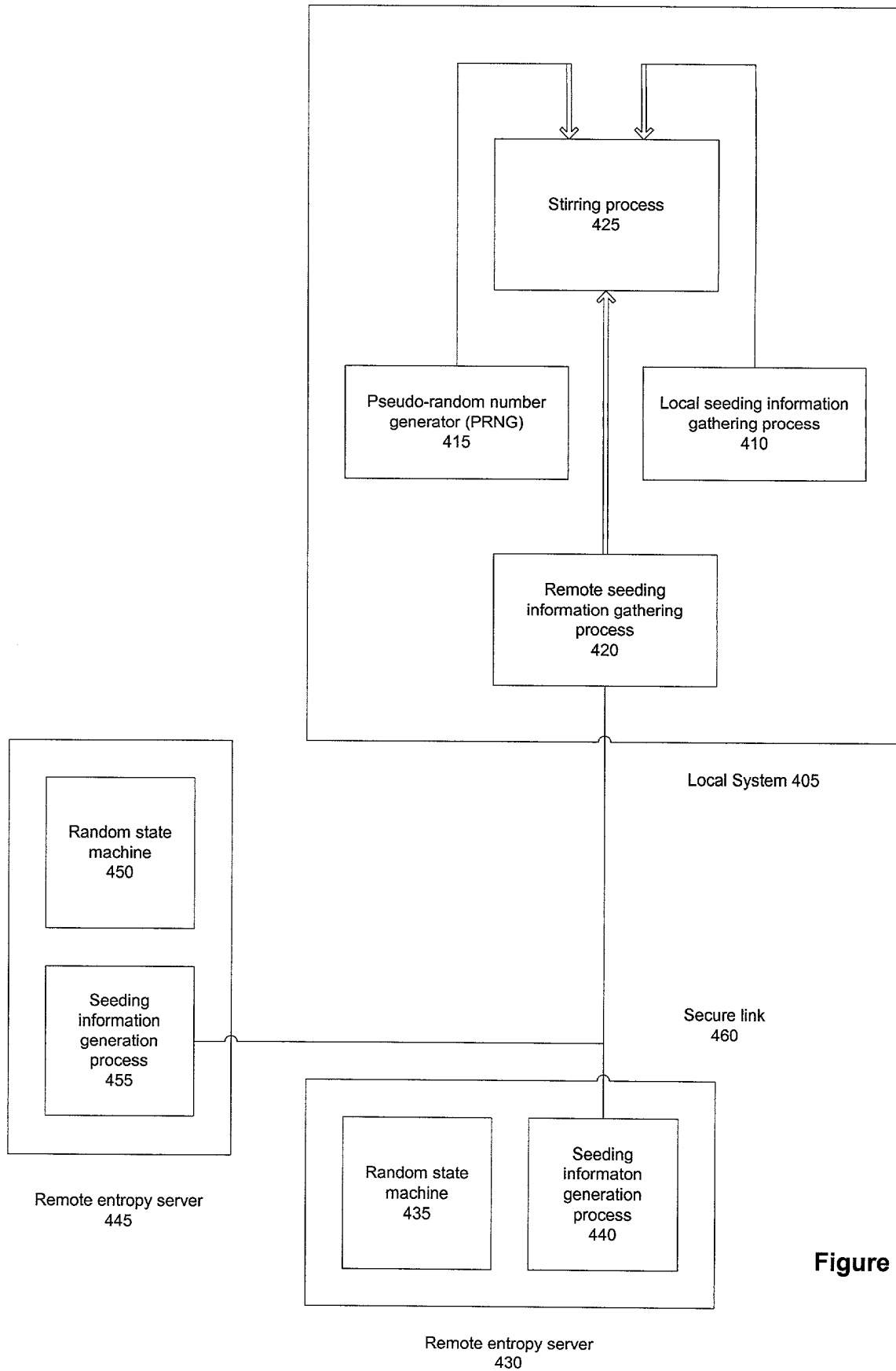


Figure 3B



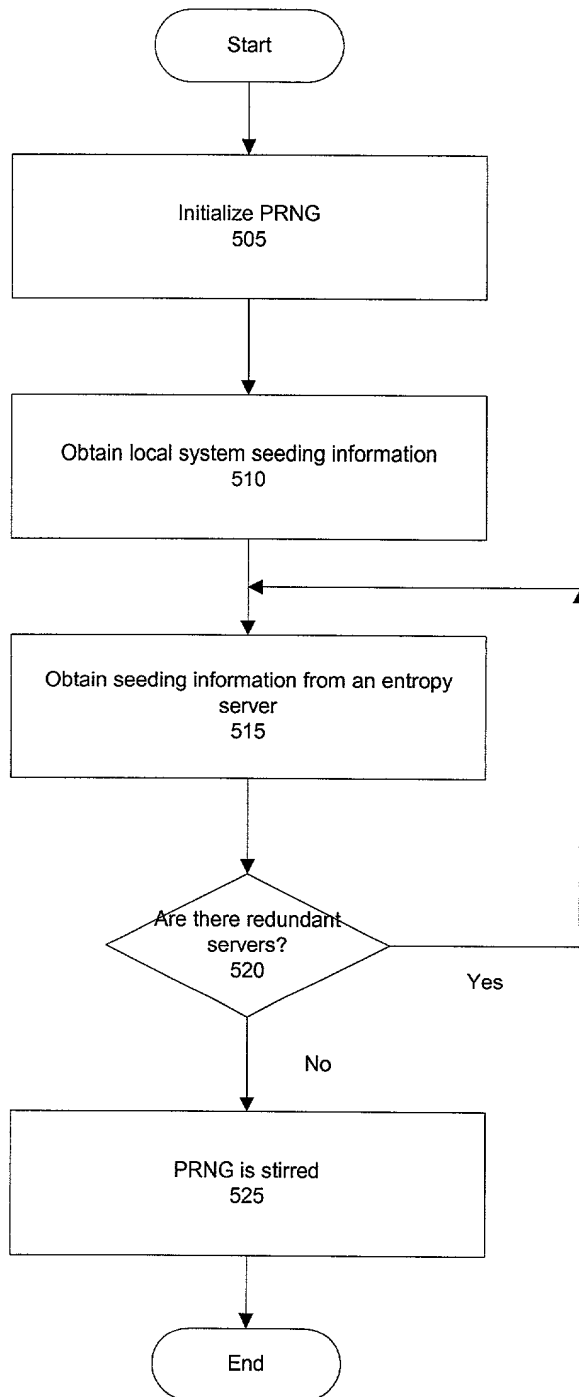


Figure 5

FIG. 6 is a flowchart illustrating a process for generating random data. The process involves a Host (600) and an Entropy Server (650) connected via a Network (695). The Host (600) generates a temporary asymmetric key pair (605) and encrypts the temporary public key with the server's public key (610). The encrypted key is sent to the server (615). The server (650) decrypts the random data using the temporary private key (640) and stirs the local PRNG using the random data (645). The server (650) also generates random data (625) and encrypts it with the host's temporary public key (630). The encrypted random data is sent to the host (635).

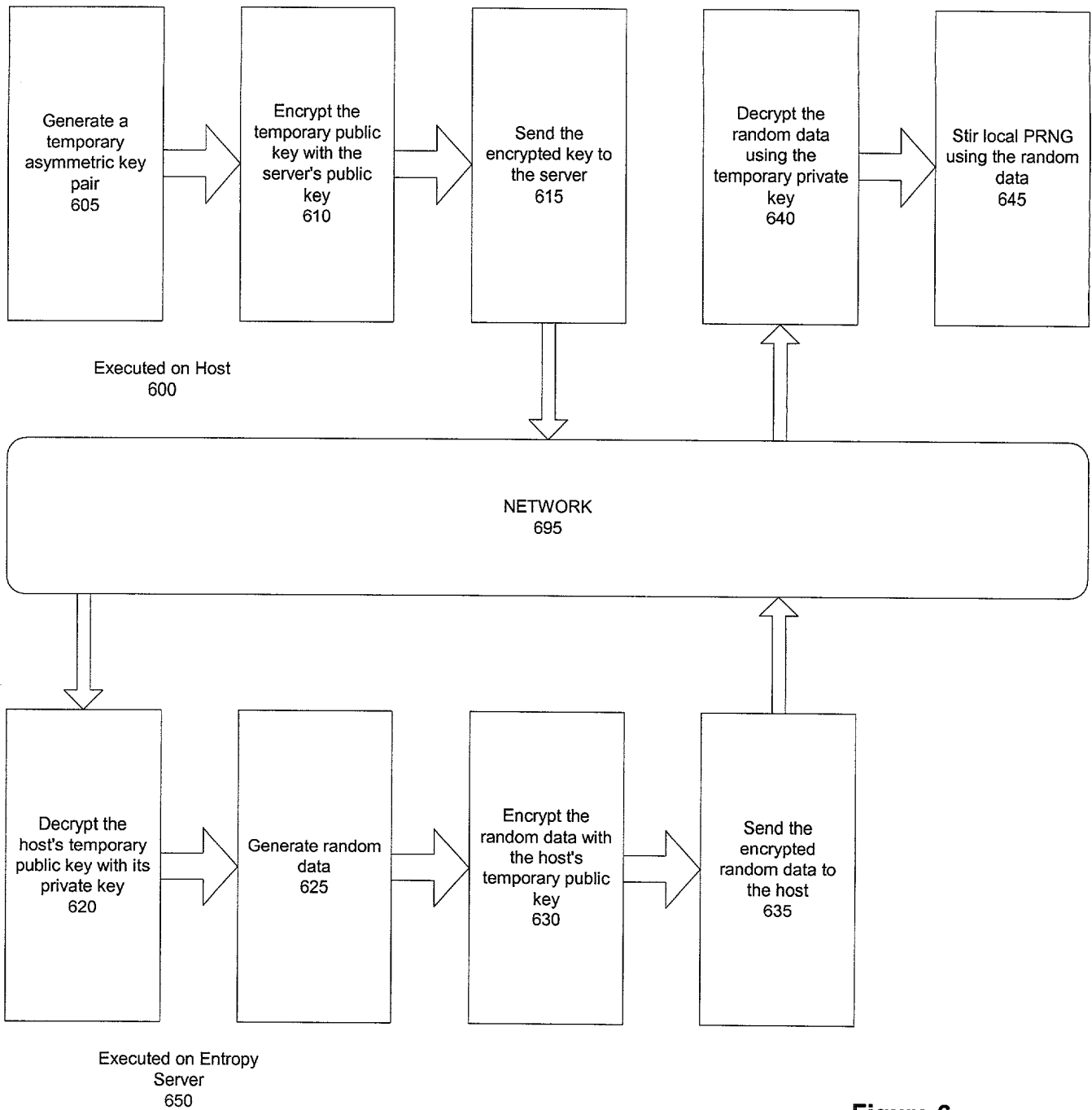


Figure 6

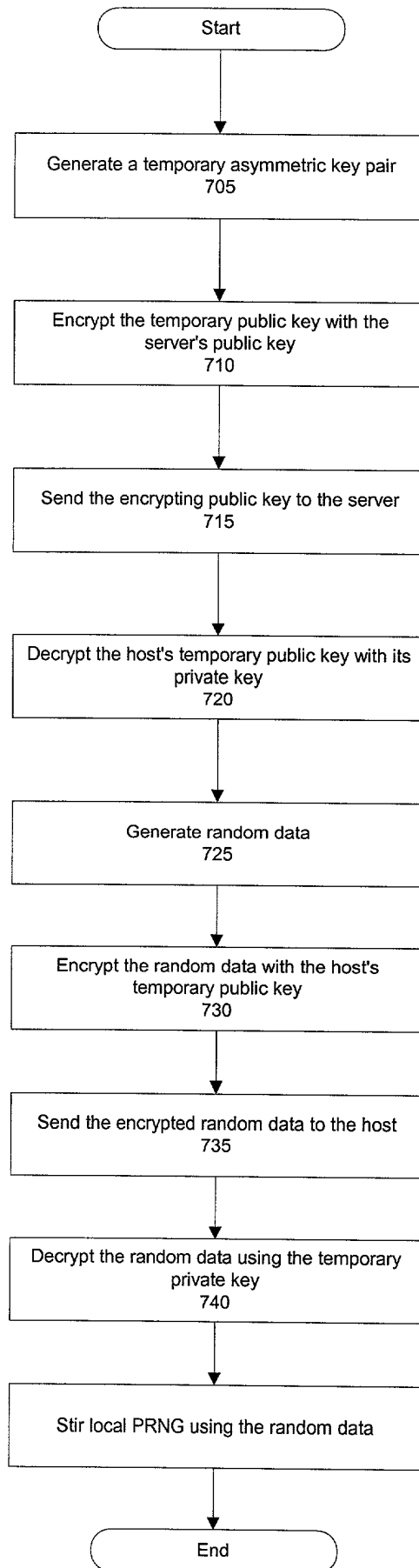


Figure 7